AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

NEW TOOLS FOR A NEW TERRAIN

AIR FORCE SUPPORT TO SPECIAL OPERATIONS IN THE CYBER ENVIRONMENT

by

Theresa A. Kopecky, Maj, USAFR

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Gregory Intoccia

Maxwell Air Force Base, Alabama

August 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

PREFACE

As a career targeteer for the US Air Force, I have focused solely on the kinetic side of the targets business. From the combat targeting desk during Operation Iraqi Freedom, to strategic targeting for US Pacific Command, the solution was always kinetic. Never before have I had the opportunity to work the other side of the coin — cyber. This research paper has been an education for me, as I explored the tactical applications of desired cyber effects for my command, Air Force Special Operations Command (AFSOC). As the world becomes increasingly connected, pulling people, objects, and places into a virtual domain where each holds a unique digital signature, I have seen the battlefield faced by my special operators shift into a five-dimensional world. Without the cyber expertise to provide a blueprint for AFSOC Cyber, this position paper is to spur thought for AFSOC and other special forces Services for the present as it can be. Cyberspace is changing, and AFSOC has the opportunity to change with it.

My sincere gratitude and thanks to my Commander, Colonel Alexander Merz, AFSOC's Director of Intelligence, Surveillance and Reconnaissance (ISR) and the wonderful folks of the AFSOC Headquarters, Intelligence Directorate (A2), especially the A2 Operations Division — without whom this paper would not be a reality, and for whom this paper was written.

Heartfelt thanks for the technical "go-to" for my husband, an Air Force combat veteran, who understood the many hours spent researching this information and the struggles to shape it into coherent thought. Finally, I would like to thank my research advisor, Dr. Gregory Intoccia, for his knowledge and assistance in slicing this overwhelming project into bite-sized pieces. My sincerest appreciation, also, to my fellow students, for their weekly dedication to help and hone each other's work. Thank you.

ABSTRACT

In a world of global interconnection, terrorists and non-state actors have increased malicious actions in cyberspace to an unprecedented level, unbound by physical geography. This paper maintains this new terrain, the cyber terrain, must be recognized and mapped for the Special Operations Forces (SOF) operator to visualize and operate within a cyberspace plane of routes, nodes, and an emerging network of physical objects with unique cyber signatures, or the Internet of Things. This new reality should change the mindset of battlefield tactics.

The purpose of this paper is to ask how Air Force Special Operations Command (AFSOC) can fulfill its mission to support the SOF operator with a range of cyber options in the battlespace environment of a cyber terrain. The research presented gives practical steps that must take place to integrate cyber effects into the AFSOC mission set, pushing cyber execution down to the tactical level and making cyber actions useable to operators on the ground and under fire. In doing so, the problem/solution framework is employed in examining the rapid globalization of cyber violence, the far-reaching effects of cyber actions, the significance of this reality to AFSOC operations, and in shaping recommendations. Measurement criteria assess three solutions: US Special Operations Command (USSOCOM) cyber targeting cells at operations centers in every theater; AFSOC Cyber Attack Teams performing live missions connected to the ground forces team in a “virtual shooter” role; and individual hand-held cyber tools for SOF teams to deliver cyber fires effects cued on target. This research finds the creation of Cyber Attack Teams can fully realize today’s need for a cyber-equipped SOF team, adept and agile in all five domains of this era’s battlefield terrain. Thus, the authority and capability to execute cyber effects at the tactical level can be a near-term reality for AFSOC and the SOF community.

INTRODUCTION

Air Force Special Operations Command (AFSOC) is faced with a unique operating terrain, cyber. As an environment in which overlapping networks exist in both physical components and non-physical elements, this cyber terrain is largely unmapped and little understood as a tactical battlefield in which Special Operations Forces (SOF) can maneuver and affect an enemy cyber persona, or digital representation of a person or entity in cyberspace. Special operations are defined as missions conducted against strategic and tactical targets to fulfill national objectives by personnel specially trained and equipped to do so.[1] However, few tools exist to aid the SOF individual, or operator, who encounters elements of cyber networks or even a cyber attack during a mission. Little is available to this SOF operator to use a construct such as a map or visualization of the cyber terrain. Few software tools exist to manipulate this "map," or visual representation of the links, nodes, and objects within the cyber terrain, to analyze and locate malevolent cyber actors present in an operating area where unconventional military operations are taking place.[2] The significance of this problem lies in the rapid globalization of the cyber network, and the escalation of cyber attacks by non-state actors. These actors are increasingly agile, requiring a swift response by a counterforce thoroughly versed in the tactics and physical behaviors of the enemy. With the right tools, the special operator could track, exploit, and protect against these violent actors in the SOF area of operations.

As a supporting command, AFSOC's mission is to provide combat ready forces for worldwide deployment, "highly trained, capable and ready to conduct special operations."[3] To fully perform this mission, AFSOC forces must be ready and able to operate in the cyber domain — using cyber tools as easily and readily as rifles and coordinated air strikes. Today, the authority and the methodology to use tactical cyber solutions on the battlefield is not fully fused

into daily AFSOC mission planning, as cyber effects are, as a rule, conducted as single events behind special access programs and generated for AFSOC by national agencies.[4]

As a result, AFSOC suffers from an inability to provide full-spectrum mission support to its direct authority, US Special Operations Command (USSOCOM) due to a lack of knowledge of cyber as a tool to be written into daily military operational plans and used in tactical engagements.[5] That required knowledge of cyber and the authority to use it resides within US Cyber Command (USCYBERCOM), the lead agency for comprehensive cyberspace defense and operations for the Department of Defense (DoD) with service elements from the Army, Navy, Marine Corps, Air Force, and the Coast Guard.[6] As such, USCYBERCOM is the strategic-level starting point for the authority, and permission, to plan and operate in the cyber realm. However, at the root of the problem is the fact that current cyber operations, especially offensive cyber operations, remain at the USCYBERCOM strategic level in planning and execution, and have not fully traced through the authority chain next to USSOCOM, and then to AFSOC for tactical execution, inhibiting AFSOC from fully supporting the SOF operator with a range of cyber options in the cyber terrain.

At the tactical level, AFSOC units have the opportunity to provide direct cyber injects into operational planning for the desired end state of, for example, the supported Joint Forces Commander or Geographic Combatant Commander.[7] Though this goal has been recognized at AFSOC Headquarters, the activity of creating targeting solutions layered with both cyber effects and kinetic effects, or working cyber awareness into daily plans, exercises, and mission execution on the battlefield is not yet taking place.[8] Hindering this ability is a lack of cyber subject matter experts, a codified set of cyber mission requirements, and a daily exercise of the cyber command channels from AFSOC to USSOCOM to USCYBERCOM. Additional tools are lacking, such as a published Cyber Joint Munitions Effectiveness Manual (JMEM) to provide

modeling, simulation, and planning tools to bring cyber munitions into mission planning.[9] Additional tools for the SOF ground team or an embedded Joint Terminal Air Controller (JTAC) are absent, such as cyber terrain modeling and cyber signature recognition, to allow the JTAC to search for and find the unique signature of a targeted physical object in the cyber domain.

For example, though defensive cyberspace operations (DCO) run on a continuing basis to protect AFSOC networks and assets, even network protection presents critical needs when AFSOC assets are deployed to austere locations with malevolent cyber actors — especially in operations requiring streaming full-motion video (FMV) of the enemy, or the interception of live foreign signals, that is, Signals Intelligence (SIGINT).[10] A larger gap exists within the realm of offensive cyberspace operations (OCO), which could be worked into every aspect of AFSOC missions on the battlefield, but are not, as indicated above. OCO could include Intelligence, Surveillance, and Reconnaissance (ISR) activities in the cyber realm, positive identification of a cyber actor, or on-demand cyber harassment of the target. Since AFSOC holds the planning authority for the missions it executes in support of SOF, this leaves a gap in planning for dominance in air, space, and cyberspace and the ability to execute cyber options at the tactical level at which AFSOC resides.[11]

In today's technologically advanced and increasingly connected world, cyber activities are already associated with nearly every daily function of US military personnel — from emails and cloud computing, to FMV data links and advanced sensors onboard US aircraft. This connectedness to the cyber realm is also true of non-US entities, including terrorists and non-state actors who engage in cyber actions on a daily basis. In answer to the need to maneuver OCO and DCO capability with ease and familiarity, Admiral Michael Rogers, the commander of USCYBERCOM, sees the future of cyberwar as being tactically executed by soldiers on the front lines using cyber-weapons as adeptly as they use live ammunition. This is the 2025 vision

of cyberwarfare — just nine years away as of the writing of this paper.[12] "In the year 2025, I believe ... Army commanders will maneuver offensive and defensive [cyber] capability much today as they maneuver ground forces," Rogers said in a 2014 interview. "The ability to integrate cyber into a broader operational concept is going to be key."[13] Neglecting the potential capabilities of a toolkit of cyber options, from hardware on the front lines to "digital reachback" relationships with USCYBERCOM, is to leave special operators on the front lines vulnerable.

In addressing this concern, this paper explores the following question: How can AFSOC fulfill its mission to support the SOF operator with a range of cyber options in the battlespace environment of a cyber terrain? This paper maintains that AFSOC can better execute its mission to support special forces individuals performing tactical operations within a terrain that contains both physical and non-physical features by integrating cyber capabilities at the tactical level.

USSOCOM, and each of its Service components to include AFSOC, must be able to effectively operate in the cyber terrain, as the unconventional enemy is increasingly dwelling in cyberspace, using it to plan, direct, and incite. AFSOC, as the Air Component to USSOCOM, has the unique knowledge to integrate cyber options at the tactical level, as the lead component for airborne ISR collection against terrorists and non-state actors. AFSOC will increasingly need to integrate cyber abilities into mission planning for validation of planning and execution authorities, means of cyber engagement, and vetting of cyber targets throughout the targeting process to eliminate collateral damage and secondary effects.

In addition, tight defense budgets and the need to create efficiencies between growing a workforce and supporting an increased demand in operations will motivate USCYBERCOM to rely on USSOCOM to work through all its Service components to perform cyber operations, to include Army, Navy, Air Force, and Marine Corps Service elements.[14] As the Air Component to USSOCOM, AFSOC can provide its unique capabilities to a cyber-focused mission for

USSOCOM, just as Air Forces Cyber (AFCYBER) does for USCYBERCOM. Therefore, with an agile force and budget, USSOCOM can play a critical role in fulfilling the mobile and tactical capabilities of both offensive and defensive cyberspace operations of the future, through the coordinated effort of its Combatant Commands, to include AFSOC.[15]

The nature of cyberwarfare is at the tipping point of change — that a tactical operator can fully immerse and engage in the full spectrum of tactics within all five domains of land, sea, air, space, and cyberspace fluidly and easily on a daily basis. This change would entail a shift from the prevailing mindset that mysterious cyber options only exist at the national agency level. Finding the means of capitalizing on the agile posture and outside-the-box thinking inherent to AFSOC will prove the significance of this study to drive new and powerful tools into the hands of the Special Forces AFSOC supports.[16]

The methodology used for this research topic will be problem/solution framework. The reader will be first introduced to the facts and assumptions surrounding the rapid globalization of cyber violence and the significance of this reality to AFSOC operations. Then three criteria will be employed for assessing possible solutions: cost, portability, and the ability of Command and Control (C2) to project to a forward location. The Mixed Methods approach used in the paper will employ both qualitative and quantitative data to measure multiple Courses of Action (COA) as solutions against these criteria. After a look into the current method for cyber integration, alternative solutions will explore: first, placing USSOCOM cyber targeting cells at operations centers in every theater; second, creating an AFSOC cyber attack team which performs live missions with the ground forces team in a “virtual shooter” role; and third, building a portable cyber tool for a ground forces team to identify targeted cyber signatures and deliver fires effects cued on target. After selecting the COA that best meets the set criteria, a vignette will be presented to illustrate the feasibility of this solution. Finally, the paper will provide

recommendations on how to implement the selected solution and final conclusions to the research.

BACKGROUND

Facts

Definition of the Cyber Terrain

The traditional form of warfare is fought in a physical plane, by individuals joined together in an organized force, with a unified purpose to either take or defend a physical piece of real estate. The Napoleonic Wars are classic examples of vast armies engaging each other upon a variety of battlefields spanning the two dimensions of land and sea. In the mid-19th century, a third dimension of warfare began to be employed in the American Civil War, by means of airborne reconnaissance balloons. By the early 20th century, mechanized warfare and the airplane were an integral part of planning and executing warfare in a three-dimensional mode. With the dawn of the space era, the tactics and use of airspace for reconnaissance, observation, and attack entered the fourth dimension of the celestial plane. Always, this multi-dimensional warfare was directly tied to a physical, geographic location on the plane of the earth and the same rules of tactics applied. Today's warfare, however, has evolved beyond all of the physical four dimensions to include the fifth dimension of cyberspace.

The US military defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[17] Cyberspace contains an overwhelming array of overlapping networks, nodes resting upon those networks, and the underlying system data that supports these networks and nodes. To break it down, cyberspace can be classified by three layers; the *physical*, the *logical*, and the *cyber-persona*. The geographic and physical components of the network through which the data travels are considered the *physical layer*. The

intangible relationships of elements in the network such as content portals on a website are considered the *logical layer*. The digital representation of a person or entity in cyberspace, that is, the people actually on the network, are considered the *cyber-persona layer*.[18] Cyberspace, then, can be thought of as a mixture of physical and non-physical elements, residing on both terrestrial and non-terrestrial planes. In a sense, military principals of war such as mass and maneuver now have considerable effect in all five dimensions. An awareness of the domain of cyber and how actions within it can produce terrestrial and non-terrestrial effects begs this question: how can tactical warfare exist in an intangible dimension?

Military tactics are historically executed within a tangible terrain, with natural features that may constitute military advantages critical to mission planning. This paper explores tactics in the fifth dimension — within the cyber domain — and the operations of military individuals and units engaging the enemy at the tactical level, that is, of or occurring at the battlefront in small-scale actions serving a larger purpose.[19] Those tactical engagements may involve a wide range of weapons, both kinetic and non-kinetic, from bullets to bombs to code. The key is to enable SOF operators to easily function in a five-dimensional world. The terrain within cyberspace those individuals must attack, take, and hold such as described in the classic land war above will not always be a physical location. Instead, it may include operating systems and software, networks, computing devices — even individuals or virtual personas.

This world of physical things, interconnected in a non-physical network is part of an emerging trend in cyberspace called the Internet of Things (IoT), that is, everyday objects with network connectivity connecting to many other different devices and accessed over multiple networks. The ability of buildings, vehicles, and nearly everything electronically-driven to send and receive data means a direct integration of the physical world into computer-based systems — truly a five-dimensional world. This world is a near-term reality, and the focus of the United

Nations' IoT Global Standards Initiative to connect the world with smart cities and communities, connecting the global infrastructure of physical and virtual things.[20] The realization of the IoT will change the mindset of battlefield tactics, most practically by knowing every physical object also has a cyber representation and signature. Mapping, visualizing, and manipulating actions both physical and non-physical is the essence of knowing the cyber terrain.

A North Atlantic Treaty Organization (NATO) study group defined the cyber terrain as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace."[21] These elements can be cataloged, measured, assessed, and, to some extent, predicted in their functions and behaviors in a similar manner as can be done against land armies of an opposing nation-state. Therefore, this language of cyber terrain and terrain mapping of cyberspace is a useful method for the US military to discuss, visualize, and operate within a cyberspace plane of routes, connections, nodes, and hot spots where personas dwell and engage in certain malicious actions.

Definition of Cyber Actors

To win a war one must know one's enemy. Understanding who lives in cyberspace and operates within the cyber terrain is key to successful military engagement. Indeed, in today's world of networked air, land, sea, space, and cyberspace operations, a thorough knowledge of the cyber terrain and cyber actors is absolutely necessary. The Federal Bureau of Investigation (FBI) defines three categories of cyber threat actors that can influence the success of the US military: organized crime groups that threaten the financial services sector; state sponsors, that is, foreign governments that engage in malevolent data pilfering from the private sector and government agencies; and thirdly, terrorist groups who use the network to exploit US critical infrastructure to disrupt and harm.[22] These terrorist cyber actors are most often non-state actors operating outside the bounds of nation-state laws and regulations.[23] Since cyberspace is, by its nature, an intangible

and unbounded area or notion, it has become a feeding frenzy of malevolent actions by these non-state actors who themselves are not bound by geographic boundaries or maps.

Taking a further look at the terrorist and non-state actors in the cyber realm, these are persons who take cyber-based actions to destroy, incapacitate, or exploit critical infrastructures achieve a political, religious, or ideological objective.[24] This often takes the form of threats to cause a fear of mass casualties, to threaten national security, to weaken the economic and financial sector, and to erode public morale and confidence in the legitimate government. Since so much of national infrastructure has become dependent on networks and computerized systems in the cyber realm, societal functions are becoming increasingly vulnerable to attack by malevolent cyber actors. This is true of transportation, telecommunications, energy, water, public health, banking, and even personal identity in a world where every physical object within the IoT also has a digital signature which can be tracked and targeted for good or evil.

Recent Trends

Predictive Trends in Cyber Warfare

Cyber warfare is a global problem.[25] The increase in the frequency and severity of cyber attacks in both the private business and military sectors is escalating into a struggle that pulls in governments, corporations, and non-state actors not bound by national borders.[26] The rapid growth of cyber espionage and hacking programs backed by nation-states, in particular, has created an emerging global cyber crisis. Some authors have used the term Code War to describe the global chaos being caused by this escalation of confusion in the digital realm. The distinguishing characteristic of this Code War is the rapid rise in cyber arms dealers trading in offensive cyber weapons, or “digital munitions.” This age of rapid development on the cyber warfront has many hallmarks of a new arms race, with a proliferation of malicious cyber code for exploitation and digital munitions, and the counter-efforts of industry partners to provide cyber target packages and enemy digital network mapping. Once, these cyber tools were close-held and

expensive secrets. Today, they are becoming accessible to non-state actors, being more readily available and cost-effective for malicious actors to purchase and use.

The Role of Terrorists and Non-State Actors

Violent extremist organizations are increasingly utilizing the cyber terrain,[27] including networking, recruiting, and communicating orders.[28] Beyond the use of networks for C2, terrorists are becoming more active in offensive cyber actions. For instance, in 2015 the Islamic State of Iraq and the Levant (ISIL) "doxed" or exposed personal identification information (PII) of one hundred US military personnel, to include their personal addresses, with messages included to attack and kill doxed individuals in their homes. As an example of the role of terrorists and non-state actors in the cyber realm, ISIL's self-declared Cyber Caliphate consists of at least three lines of effort: disrupt broadcasts by gaining control of media systems; acquire access to US government or adversary websites and social media to deface and recruit; and dox US military personnel to make them vulnerable as targets for ISIL sympathizers.[29]

Just as non-state actors have transcended national state boundaries in their effect and their reach, so violence instigated in the cyber realm has crossed to the physical environment by delivering kinetic-like effects in its capability to destroy.[30] Violent acts that originate from cyber actions range across the spectrum from electronic jihad (e-jihad) rhetoric and psychological operations influencing emotions and behavior, to a physical computer network attack (CNA). Cyber warfare offers speed and anonymity, making it difficult to distinguish between actions of terrorists, non-state actors, criminals, and nation states.[31] The seriousness of the trends in cyber attack lies in the fact that a cyber attack on certain information networks can actually cause loss of life. This could include anything from getting in and changing a pharmacy's patient prescriptions to manipulating settings on dams or electrical power distribution grids.

Significance of the Problem

Increasing Importance to Air Force Special Operations Command (AFSOC)

The DoD Cyber Strategy, published in April of 2015, issued the strategic goal of integrating cyber operations with those in other warfighting domains, citing a deficiency in defining specific cyberspace effects against targets.[32] The first step of this multi-domain integration is to realize the severity of cyber violence and recognize that military operations can be planned and executed in the cyber terrain just as they are in any other terrain.[33] USCYBERCOM has defined cyber terrain as "those physical and logical elements of the domain that enable mission essential warfighting functions."[34] For the tactical warfighter, understanding the key cyber terrain, and knowing how to map and visualize it with operational and intelligence injects to create a comprehensive construct of the enemy is critical to that enemy's defeat.

AFSOC's mission scope is to support SOF through all Air Force dimensions of air, space, and cyberspace.[35] Effective employment and mitigation in the cyber environment requires an understanding of the targeting process and policies, the cyber enterprise, and an exploration of its possible application on the cyber battlefront.[36] Employment of any type of tactical cyber effect requires a knowledge of command relationships and ultimate decision authority to authorize cyber actions. A key part of this authority for AFSOC to execute cyber effects in support of the special operator will be the ethics, laws, and consequences of offensive cyber actions — the political ramifications, and collateral damage concerns.[37] The increasing amount of guidance, regulations, and policies governing actions in cyberspace will be a key part of mission planning for AFSOC.[38]

This total picture of the cyber terrain, both physical and non-physical, will characterize key features of the environment in which the tactical operator must make cyber decisions.[39] As AFSOC steps into this cyber terrain in its supporting mission to SOF, it will need to recognize, track, and defeat such targets as cyber personas as adeptly as it does high-value individuals.

Emerging Solutions to the Problem

A review of current solutions reveals other US military services are taking steps to solve this problem. To counter the increasing threat to US systems, weapons, and people that exists in the cyber terrain, Lieutenant General Cardon, the commander of U.S. Army Cyber Command (ARCYBER), has pushed for Army initiatives in cyber network mapping as well as cloud and virtualization — key elements to produce a useable map of the cyber terrain, and in step with the National Geospatial Agency's (NGA) effort for geo-rectified cyber mapping, that is, to project a digital representation of cyber activity onto a geographic map.[40] ARCYBER is also closely involved with the Defense Advanced Research Projects Agency (DARPA) on its Plan X Cyberwarfare Program to provide tactical operators on the battlefield with a visualization of the cyber threats they encounter while conducting a mission on the ground.[41] Moreover, this technology allows the operator to identify elements of key cyber terrain, and then plan missions and execute cyber effects by punching up "apps" to perform the cyber function required.[42] This is only the latest in DoD and Joint Service efforts to push cyber down to the tactical level and make cyber actions useable to operators on the ground and under fire.

For USSOCOM, these cyber threats as detailed above are increasingly a part of unconventional strategies essential to SOF operations. As the outgoing USSOCOM Commander, General Joseph L. Votel, stated to Congress regarding cyber for SOF, "It is time for us to have an in-depth discussion on how we can best support our national interests in these situations."[43] This research paper presents a new perspective to the practical steps that must take place to integrate tactical cyber effects into the AFSOC mission set to support SOF operations.

THE CURRENT STATE
Current Solutions

Before alternative solutions and future recommendations for AFSOC can be discussed, the current status of military doctrine on cyberspace operations must be explored. The C2 relationships between national agencies and the component commands for conducting actions in the cyber domain are a balancing act between degrees of control. The Commander, USCYBERCOM, manages day-to-day global cyberspace operations, while the theater commander, or Geographic Combatant Commander (GCC) is the supported commander for any first-order cyber effects within the GCC's area of operations. If that cyber action crosses boundaries into a transregional or global effect, the authority reverts back to USCYBERCOM.[44] Similarly, USCYBERCOM grants to the GCC cyber experts and teams by using the construct of a Command-level Joint Cyberspace Center (JCC) and theater-level Cyberspace Support Elements (CSE). These CSEs are made up of USCYBERCOM forces and are deployed to the GCC to provide cyber subject matter expertise and planning, to include building cyberspace requirements. However, the CSE personnel are merely "on loan," as USCYBERCOM retains operational control of them.[45] The CSE reports directly to the Command's JCC, who ensures all cyber effects are constrained within authorized parameters.[46] The JCC also works with USCYBERCOM to bridge the gap between strategic knowledge held at USCYBERCOM and the tactical knowledge of networks in theater to provide the GCC a tailored understanding of the local battlefield.[47] In theory, the local commander, with tactical knowledge and mission needs, can use this C2 framework to channel a tactical cyber request from the local CSE, through the JCC, and to USCYBERCOM for support. However, this C2 construct is not currently answering the mission needs of AFSOC.

The leadership of AFSOC has recognized the need for greater integration of cyber capabilities in AFSOC mission planning, pushing for greater cyber scenario injects into major Joint Service exercises and making cyber mission capability a priority.[48] In fact, at AFSOC Headquarters in Hurlburt Field, Florida, the directorates of Intelligence (A2), Operations (A3), and Communications (A6) have created an AFSOC Cyber Team, or ACT, with a mission statement to "build the capacity in AFSOC to maintain advanced awareness of threats and the ability to plan for and request cyberspace effects to support Air Force Special Operations Forces (AFSOF) missions."[49] This fledgling team, created earlier in 2016, seeks to bring cyber expertise to AFSOC in order to better support its parent organization, USSOCOM, in USSOCOM's own creation of a Joint Cyber Cell (JCC).[50] In the hierarchy of the chain of command, it is the goal of USSOCOM's JCC to better support the cyber activities of each of its Component Commands, to include AFSOC. In turn, AFSOC is seeking USSOCOM's support of cyber mission requirements — once those are fully defined for AFSOC units.[51] The vision of both AFSOC's ACT and USSOCOM's JCC is to create synergy between those units and individuals actually planning and executing missions, and the higher headquarters that support them.[52] At the present time, this decentralized execution of tactical cyber options at the unit level is only a dream sheet or wish list.

Opposing Viewpoint: Centralization of All Cyber Operations

Argument For Centralization

The biggest question the US military has struggled to answer regarding tactical cyber has been how much to decentralize to the tactical or unit level. USCYBERCOM has been given the authority to manage, plan, and execute all things cyber. The counterargument to this paper's conclusions regarding decentralization is to continue to allow USCYBERCOM to centralize cyber decisions and maintain control of dedicated cyber mission teams and the conduct of offensive cyber actions.[53] In fact, USCYBERCOM is currently building such teams with a three-

part mission to defend national infrastructure, protect DoD networks, and conduct cyberspace operations to achieve combatant commander objectives.[54] These new cyber mission teams, to be completed by 2018, are self-contained units that are Service-specific, pulling dedicated forces from each Service component.[55] Where the CSEs originally provided by USCYBERCOM could not command and control forces, these cyber mission teams are squadron-sized basic fighting units. Offensive cyber actions in this construct will be conducted by the "combat mission force," dedicated by USCYBERCOM to conduct cyber operations on behalf of the combatant commanders.[56] For SOF, this would mean that any tactical cyber actions or needs would be apportioned directly to USCYBERCOM via its combat mission force.

The more USCYBERCOM defines its mission and grows its force and reach into direct tactical actions, the greater the cry becomes for a separate Cyber Service.[57] With the rapid globalization of cyberspace networks, actions, and violence, some officials say a Cyber Service would be able and equipped to handle the specific mission set of this cyber domain in much the same way that the Air Force focuses on air superiority.[58] A separate Cyber Service, in this argument, would also allow for specific mission planning and remove the complicated C2 channels that exist for cyber operations across the Services, as described above. In fact, the move by USCYBERCOM to create these new cyber mission teams that peel off dedicated Service members and specific mission sets can be seen in this light of a separate Cyber Service. While it is not within the scope of this paper to argue for or against a Cyber Service, the fact remains that some believe USCYBERCOM should centralize cyber actions to its own authority and control.

Argument Against Centralization

In essence, AFSOC is currently operating under a de facto centralization of cyber operations for its mission planning. Indeed, current solutions for AFSOC cyber mission planning include working through USCYBERCOM to pre-plan months in advance or requesting

compartmentalized operations through channels within the AFSOC Operations Division. These options involve a long lead time, a considerable effort to up-channel requests through proper authorities, and the difficulties in working sensitive and classified information into mission plans of a lower classification level. If the individuals who must execute the mission cannot talk about the plan or see what the plan looks like, it becomes increasingly difficult to integrate cyber planning into a robust, daily effort.

In a forward-deployed capacity, AFSOC personnel often must work with outside agencies to share and disseminate ISR information. For instance, an operations center may have SIGINT and FMV data received from the AFSOC airborne assets overhead. As items or persons of interest are picked up, the AFSOC personnel working at the forward-deployed operations center may need to cross-cue this data with the National Security Agency (NSA) or USCYBERCOM to positively identify the observation, to track it, or to exploit it. In such situations, mission success is often dependent on the abilities of the individuals deployed together to make it happen and draw solutions from the assets and capabilities at hand. This on-the-fly mission adaptability has been key to innovative solutions within the existing framework of USCYBERCOM and NSA authorities to operate, by USSOCOM and AFSOC individuals deployed to forward-based units or operations centers. However, this solution is fleeting and dependent on having the right person at the right desk at the right time.[59] To remedy this lack of formalized tactics, USSOCOM and AFSOC are working to better integrate cyber effects and missions with a cyber focus into current Joint SOF exercises with real-time, on-target cyber support for tactical objectives.[60]

ALTERNATIVES

This research paper presents three alternative Courses of Action, or COAs, to build the authority and capability for AFSOC to integrate tactical cyber effects into its mission. Each of

these COAs takes this cyber integration in different directions to explore a range of cyber options and methods of change.

Mission Criteria

Any proposed change to AFSOC's mission capabilities and priorities must be weighed by a cost versus gain analysis. To provide an objective measurement standard and determine AFSOC's best way forward, three mission criteria emerge as key elements to a successful strategy to provide the SOF operator with a range of cyber options in the cyber terrain. These three criteria are: cost-effectiveness, C2 capability while forward-deployed, and portability. Taken together as mission-essential behaviors of how AFSOC conducts business, these three criteria provide an objective measurement standard to weigh the feasibility of three possible alternatives to the current solution, and reveal the best course of action.

Cost-Effectiveness

Solutions that include cyber effects into current and future mission planning need to be cost effective and do much with little. A comparison can be drawn between two Major Commands (MAJCOM) in the United States Air Force with similar mission statements for on-demand global presence — AFSOC and Air Mobility Command (AMC). AMC's mission is to provide global air mobility, "right effects, right place, right time," to include assisting with special duty and operational support aircraft when called upon to do so.[61] Like AMC, AFSOC has a global mission, with the requirement of being ready to support operations "anytime…anyplace," as given in AFSOC's mission statement.[62] What illustrates AFSOC's absolute necessity for cost-effective solutions is the fact that AFSOC must fulfill this global mission with a force of only 19,500 active-duty, Air Force Reserve, Air National Guard, and civilian personnel, as compared to AMC's 126,000 total force personnel.[63]

As a relatively small command, AFSOC is required to support Special Forces with short to little notice tasks anywhere on the globe with an agile, lean force. To accomplish this, AFSOC has learned to do much with little in terms of resources, manning, and budget, especially in today's fiscally lean times. This challenge has created a can-do atmosphere within the command, as units and individuals have adapted the tools and resources available to do more with what they have. "Get the job done" has become the motto. Therefore, cost-effectiveness is a key criterion in any consideration of pursuing a tactical cyber effects solution. AFSOC needs to use what it already has, in terms of people, systems, C2, and perhaps even organizational schemas because there is little budget for a large-scale overhaul of personnel, training, and gear.

Forward C2 Architecture Capability

The "tip of the spear" is a term often used for Special Forces, referring to the first soldiers to go into a war zone, or for those who infiltrate behind enemy lines for secretive and dangerous missions that are key to the overall battle's success.[64] This ability to project power forward, far from base support, is a critical part of AFSOC's global, on-demand mission. The reality of today's networked operations — linking communications, geolocation, signals, and flight plans into data streams that rest in cyberspace — requires a secure and safe network. This is especially true of operations that are projected forward, in regions of degraded communication ability in mountain ranges such as Afghanistan, or in areas of increased threat of cyber attack and exploitation such as Syria.[65]

AFSOC must seamlessly manipulate all elements of Command, Control, Communication, Intelligence, Surveillance, and Reconnaissance (C3ISR) in any notional mission in a forward-deployed environment. A typical FMV mission scenario that practices the elements of C3ISR may run like this: an MQ-9 Reaper takes off from a forward operating base in Afghanistan. The mission profile and flight plan are logged and sent via email to the units working the mission.

The MQ-9 takes off, en route to a valley high in a nearby mountain range. During the flight, the cameras on board are viewing and recording FMV and sending that signal back to an operations center via global positioning system (GPS) satellite signals. The operations center analyzes the FMV feed and provides intelligence data on what they see and what it means. This is relayed to the SOF operators who may initiate a direct action mission to engage the target, based on the intelligence findings and a "go/no-go" call from higher authority via C2 channels. This notional scenario illustrates the role that GPS and web-based communications play in a successful AFSOC mission. It also provides key points as to the necessity of any tactical cyber solution deployed forward to be secure from exploitation or attack, to work under a degraded C2 environment, and to be robust enough to carry sophisticated signal data, such as identifying and relaying cyber signatures within the area of operations. Therefore, a capable C2 architecture while forward-deployed is a key factor in analyzing possible cyber solutions for AFSOC.

Portability

Portability is the third key factor to weigh possible solutions for AFSOC in providing cyber effects in its support of special operations. Whether installed on a light, small-frame aircraft or clipped to the personal gear of an AFSOC Combat Controller deployed with an Army Ranger team on the ground, any physical solution must keep in mind weight and size restrictions. Size, weight, and power (SWaP) must be kept to a minimum, while the performance of a solution must increase in capacity, reliability, and capability when upgrading systems.[66]

The Combat Controller provides a good example of the necessity of portability to any cyber solution. Combat Control Teams (CCT), singular Combat Controller, are a part of AFSOC's Special Tactics Squadrons providing air support coordination to special operations ground forces.[67] The Combat Controller's mission is to deploy undetected into hostile areas, provide reconnaissance and forward air control, while also deploying with air and ground forces

in support of direct action missions. Many Combat Controllers qualify as Joint Terminal Attack Controllers, or JTACs, and perform functions such as calling in and directing precision air strikes, close air support to the ground team, and fires support.[68]

As a light, agile presence, CCT or JTAC personnel going in can only take what they can carry, which typically consists of secure satellite communications, infrared lights, strobes, and laser target designators in addition to personal gear and munitions. On the airborne side, AFSOC uses small, light airframes in many instances, such as the Pilatus PC-12 airframe, designated the U-28A, which is often maxed out with a long list of already-necessary gear, sensor suites, and communications antennae for its robust datalink.[69] This illustrates the criticality of a portable solution, since for many missions a Combat Controller embedded with a SEa, Air and Land (SEAL) team on the ground or a U-28A airborne over the deserts of Africa has little capacity to add another piece of equipment to the list.

Alternatives

After an extensive look into the background of the escalation in cyber violence, the proliferation of networks and nodes, the increasing connection of physical objects into an Internet of Things, and the current status of AFSOC mission capabilities, this paper presents three alternative solutions, or COAs, to enable AFOSC to fulfill its mission to support the SOF operator with a range of options in the cyber terrain. Each COA will be assessed by the three measurement criteria of cost-effectiveness, C2 capability, and portability, revealing the best way forward for AFSOC to fulfill its mission to support the SOF operator in the cyber terrain of today and the future.

Course of Action (COA) 1: Cyber Targeting Cells at Operations Centers

The first alternative that should be considered would place USSOCOM cyber targeting cells at operations centers in every theater of operation. In this COA, USSOCOM would have a

team of embedded cyber subject matter experts, made up of personnel from USCYBERCOM, NSA, USSOCOM's JCC, and representatives from USSOCOM's Service Components to include AFSOC. In this construct, this Joint Cyber Targeting Cell, or JCTC, is sponsored by USSOCOM, and the personnel within it fall under the command authority of USSOCOM itself. In contrast to the CSEs described above which belong to USCYBERCOM but which are "on loan" to the combatant commands, this JCTC would be created by SOF for SOF. The mission capability of the JCTC would be similar to the CSEs, in that the JCTC would provide the cyber subject matter expertise, work cyber effects into mission planning, ensure cyber effects are conducted within mission parameters, and build cyberspace requirements.

This JCTC idea uses a C2 framework that currently exists for USSOCOM's theater or forward-based operations centers. Theater Special Operations Commands (TSOCs) reside at each of the geographic combatant commands and are responsible for employment of forces, assigning objectives, and executing the mission.[70] Typically, USSOCOM assigns one to two personnel to each TSOC as the cyber subject matter expert. However, the ability of these individuals to plan robust, daily cyber effects into the TSOC mission, along with the permissions and authority to execute these effects, is not currently occurring for the combatant commander at this level.[71]

A look at the conventional forces' Air Operations Center (AOC) can illustrate and fully expand the possibilities of placing USSOCOM Joint Cyber Targeting Cells at operations centers. An AOC exists to provide the Air Force component commander with a C2 center to plan, direct, and execute missions with assigned and attached forces, similar to a TSOC.[72] The AOC is the hub of ongoing operations for conventional forces, with distinct divisions that plan strategy, task forces, and send aircraft out to put bombs on target. To do so, the AOC contains liaison elements from each of the Services, as well as each of the functions, such as targeting, information

operations (IO), cyber, space, and weather, to name a few. USSOCOM has a liaison at the AOC, as well, the special operations liaison element (SOLE), which works to coordinate, deconflict, and synchronize SOF activities and fire support.[73]

A proposed scenario placing a notional JCTC within an AOC would involve inserting a team of SOF cyber targeting specialists as liaisons alongside the SOLE during ongoing current operations. This JCTC would have the task of working cyber effects into the mission planning cycle, just as is done for kinetic and IO effects. The timeline of this mission planning should be comparable to the kinetic Targeting Desk, and would have the same type of pre-planning needs, such as running computer-based scenarios of the first-, second-, and third-order effects of the strike, modeling of any potential collateral damage, and an assessment of the best tool or option to create the desired effect in the commander's guidance and intent. In addition, the cyber targeting solution presented by this notional team would be presented to the Judge Advocate General (JAG) for clearance of the targeted object and the desired force.[74] USSOCOM's JCTC would then execute and assess the mission.

In comparison, a JCTC located at the TSOC, and executing missions directly for the GCC, would mirror the roles and responsibilities in the AOC illustration above. Here, C2 authorities would reside at the combatant command, with a direct link through USSOCOM back to USCYBERCOM for authority and technology to operate and conduct cyber strikes. In theory, the approval process to be cleared to engage in a cyber strike would mirror the kinetic strike approval process, which runs from the Combat Targeting Cell at the AOC to the national command authority for President of the United States (POTUS) approval to engage the target. Thus, the timeline and authority to strike during ongoing tactical operations would be streamlined by the inclusion of USCYBERCOM and NSA individuals in the proposed JCTC.

Cyber-based firepower, as planned and executed by the JCTC, can enhance kinetic weapons with kinetic impacts by honing in on the digital signature of the target and allowing the ground team to physically shoot the target. Conversely, this cyber-based firepower can be used to have cyber impacts only, with operations that begin and end in cyberspace. Therefore, these cyber operations would be categorized into two types; operations whose effects remain in cyberspace and operations that begin in cyberspace but have kinetic impacts.

It would be helpful to use the SOF targeting mnemonic "find, fix, finish" to describe the difference between these two operation types. An operation that is initiated in cyberspace to find the digital signature of a terrorist media center, then to fix on to the media center's systems and hack into them, and finally to burn the target and finish it using code is an operation completely conducted in the fifth dimension of cyberspace. An operation that uses airborne ISR sources to find a targeted individual using visual confirmation via FMV, then uses cyber capabilities to fix and confirm a digital match to the handset of the individual and steal the data on that handset, then finally calls in an airstrike to put physical bombs on target to finish it, is an operation that blends behaviors in all five dimensions of warfare. This type of operation relies on a variety of capabilities to find, fix, finish the target and produce the effects required by the commander's intent.

Whether located at an AOC or at the TSOC, the JCTC would make extensive use of the Cyber JMEM as it prepares its cyber targeting solutions, just as is done for kinetic targeting solutions. The cyber target system would be studied in coordination with NSA and USCYBERCOM and authorized as a valid target by the Joint Targeting Board, USCYBERCOM, USSOCOM, and the JAG. The cyber target system and the designated target points would undergo modeling and simulation by the mission planners to anticipate second- and third-order effects of the cyber strike. A Collateral Damage Estimate (CDE) algorithm and CDE modeling

software would be created in coordination with the Cyber JMEM to give the best predictions for each offensive cyber action, as protective measures to ensure that tactical cyber operations do not quickly become strategic concerns.[75]

The CNA Risk and Effectiveness Analyzer (C-REA) is an example of software that can be used to support this COA to calculate predictive assessments. The C-REA uses logic models to display risk and effectiveness for cyber operations, even showing the points at which the mission plan should mitigate risk of adverse outcomes.[76] This type of modeling and simulation would aid the JCTC in making final mission recommendations to the mission commander. Pre-operation steps such as these are carefully scripted for today's kinetic strikes — tactical or strategic. This COA, as well as the alternative COAs which follow, anticipates that a pre-operation script on the cyber side would be just as deliberate, and that accurate modeling, simulation, and approval would be an integral part of every tactical cyber strike.

COA 2: Tactical Cyber Authority Decentralized to AFSOC Units

The second COA for consideration would see the formation of Cyber Attack Teams, or CATs, for AFSOC units, headquartered at Hurlburt Field, Florida. These teams at the squadron level would break new ground by bringing the fifth dimension of cyber directly onto the special operations battlefield by performing tactical targeting and releasing cyber munitions in direct support of individual special operations missions.

In this COA, AFSOC would stand up proposed teams composed of assigned AFSOC individuals from the A2 Intelligence, A3 Operations, and A6 Communications directorates in a variety of career fields, including, but not limited to, cyberspace operations, intelligence, aircrew operations, command and control systems operations, and special tactics. This notion is based on the concept that tactical cyber authority can and should be decentralized to the lowest level of execution, in this case, to AFSOF. Working back up the chain of command, these CATs which

reside at AFSOC's tactical execution level would rely on strategic and operational direction from USSOCOM, the supported command. As the Air Component, AFSOC would remain lock-step with USSOCOM's JCC as it works to integrate cyber effects into every aspect of mission planning for each of the SOF Services, as an integral part of every SOF mission on the battlefield of the future.

This COA to create a CAT construct would generate the cyber-focused personnel, equipment, and expertise to join the AFSOC team going out in direct support of a SOF mission. In execution, this CAT would function as a "virtual shooter" by providing real-time mission-focused cyber-based firepower to affect the enemy and shape their actions, in somewhat the same manner as other fire support assets. As the virtual shooter, the CAT would remain connected to the ground team via a robust data link on the gear of an individual such as the CCT or JTAC. Throughout the mission, the CAT would remain "live" with the team and employ cyber weapons to affect the enemy during the attack, just as any other member of the ground team would use covering fire or a feint.

In fact, the CAT also needs to be an integral part of the Joint mission planing process. In essence, the CAT is about getting inside the OODA Loop of the enemy — that is, the enemy's decision cycle of observe, orient, decide, and act — and getting the enemy to do what the mission commander wants him to do, at a time and place dictated by the mission. In bringing tactical cyber effects into the mission planning process, the CAT is inserting the fifth dimension into the planning cycle as scoped at the strategic and operational level by AFSOC's parent organization, USSOCOM, and by the Joint Force Commander at Joint Special Operations Command (JSOC). The CATs, located at the AFSOC squadrons, would stay connected to the heartbeat of USSOCOM and JSOC cyber plans through the Cyber Targeting Officer (CTO) already sketched out in USSOCOM's JCC organizational chart. This CTO would exist as an

integral part of the cyber mission planning process, both aiding and guiding the tactical activities of AFSOC's CATs.

In cyber terms, this COA proposes the employment of virtual munitions during an operation which are tailored to create a range of tactically useful effects. These cyber effects would range from instilling general confusion at critical moments by degrading a targeted organization's security and communication systems at a specified time-on-target, or by initiating highly tailored virtual fires designed to affect the target's actions in specific ways during the time period of the operation. Shaping the target's actions would involve spoofing to cause the system to open or close certain physical doors for the ground team to go in, or to open or close digital ports to allow the CAT to manipulate the functions of a building at will, such as temperature, lights, cameras, or security logs. This virtual ammunition would be delivered to the end user by means of an "app" on an open architecture framework, which the CAT would release upon order during the live mission, either in response to a designated time-on-target, or on-call as cyber "air support."

The virtual ammunition used to create these cyber effects would require the liaison activities of the CAT and USSOCOM's CTO at its JCC in order to integrate cyber pre-planning into every aspect of the mission plan. When a traditional Joint SOF operation calls for an AC-130 gunship squadron to provide "air support" to the ground team, the AFSOC squadron providing that aircraft conducts mission planning using its own organic resources. In contrast, highly tailored virtual fires providing cyber support for the ground team would require the AFSOC CAT team executing that tactical support to be tightly connected with the CTO on USSOCOM's JCC, and to work closely with national agencies to script and pre-plan the cyber options for the team — later to be used as "apps" on the battlefield.

In this COA, the scope of such CAT cyber actions would align with the same guidelines and rules of engagement as the rest of the mission plan, as directed by the mission commander. So as to circumvent or anticipate second- and third-order effects, the mission planning process would perform modeling and simulation for the chosen weapon system, whether kinetic or non-kinetic, as well as review by the JAG, just as described above in the first COA. Since the CAT is an integral part of the AFSOC team in support of the ground forces mission, the cyber activities of the CAT would be vetted as part of the mission planning process adhering to these careful processes.

Any cyber effects to be used in the mission would be carefully scripted and authorized prior to use, using simulation software to circumvent the law of unintended consequences as much as is humanly possible. Far reaching effects are taken into consideration during current mission planning as a part of creating the best effect, kinetic or non-kinetic, to answer the commander's intent. Cyber mission planning for the CAT would be just as focused, and would also adhere to the targeting principles of an effects-based approach to operations (EBAO) and the targeting cycle.[77]

It would be useful to present a practical corollary drawn from current AFSOC operations to illustrate how this proposed CAT may operate. Earlier in this paper, a notional MQ-9 Reaper mission profile detailed the necessity of a robust forward-deployed C2 architecture to handle ISR findings. Within that same example, as the MQ-9 is flying above that little valley, the onboard sensors are imaging and recording FMV of the local area and relaying it in near-real time to an intelligence squadron with experienced personnel to view, interpret, and disseminate their findings. These findings are relayed back to the ground forces team, perhaps through a JTAC embedded with the ground team. When the FMV reveals a gathering of individuals at a known enemy weapons cache, and the intelligence professionals interpreting and cueing the FMV data

confirm that the target has arrived on the scene, a trigger event occurs, and the ground team goes into action, perhaps calling in an air strike to eliminate the target and the weapons cache.

In this illustration, AFSOC provides direct support to SOF teams on the ground, executing a coordinated mission. In a notional Combat Attack Team, the CAT is more — a shooting member of the SOF team. In consequence, the CAT is a part of the entire planning process of a given mission, being the subject matter expert in cyber effects and pulling reachback support from USCYBERCOM or NSA via the CTO at USSOCOM's JCC. In addition, just as AFSOC can contribute a JTAC individual to the SOF team executing the mission on the ground, similarly, the CAT virtually "goes in" with the SOF team, and performs as a participating member of that team. Looking back at this scenario of an emerging event occurring on the ground, perhaps neither the FMV analysts nor the ground team can confirm that the man arriving on the scene is the one they are after. Instead of watching the target walk away from the scene, the CAT might pull up the known handset number of that individual, cause the handset to ring, and produce a positive identification of the individual to trigger the operation, bringing the mission to success within moments.

The creation of a CAT as a virtual shooter and member of the ground forces team begins to bring tactical warfare into all five domains simultaneously. In following the growth of cyberspace and the enemy's increasing use of force in the cyber realm, as described earlier in this paper, the concept of the CAT as a virtual shooter pulls modern tactics into the fifth dimension. The CAT, as fully integrated into mission planning and execution brings the future of cyberwarfare to today's fight, putting cyber-weapons on the front lines to be tactically executed by ground forces as adeptly as live ammunition. The actions of the CAT are in line with this vision as expressed by the USCYBERCOM commander, Admiral Michael Rogers, and takes the

recent efforts of AFSOC leadership as detailed above to create the AFSOC Cyber Team to the next level.[78]

COA 3: Hand-Held Cyber Tools Included in Joint Terminal Attack Controller (JTAC) Gear

The third, and final, COA for consideration is to put hand-held cyber tools into the equipment of AFSOC personnel embedded in the ground forces team. AFSOC would initiate a research program to craft a capability to put cyber actions and decisions directly into the hands of the team on the ground, leveraging current efforts in government, industry, or university to build new technologies. The CCT or JTAC, for example, would carry a hand-held device with pre-loaded "apps" necessary for a given mission, and then deploy these cyber actions at certain execution times within the mission profile. Drawing parallels between cyber fires and kinetic fires, this COA would give the special forces operator a tactical cyber weapon just as functional as the other weapons carried upon their person.

SOF already uses wearable technologies. For example, the Modular Tactical System (MTS) is an integrated multi-mission system used by Special Forces in battle that pulls data from radios, digital signals, and computing devices and funnels them to a central display housed in the plate carrier of a tactical team member.[79] By 2017, AFSOC should begin fielding an adaptation of the MTS system, called the Battlefield Air Operations Operator Control System (OCS). This OCS makes the JTAC or CCT a walking computer, bringing precision-strike and C2 solutions directly to their fingertips for a truly foot-mobile solution.[80] Germaine to a cyber hand-held tool, the OCS will give an AFSOC operator the ability to provide tactical communications for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), digitally aided close air support (DACAS) operations, and small unmanned aircraft system (sUAS) control.[81]

As an example, the JTAC on the ground would use the OCS wearable kit to control an sUAS with a SIGINT sensor suite to find, fix, and track a desired cyber signature. Once a positive identification has been made, the JTAC would then either use the DACAS function to visually depict the targeted area and call in an air strike, or initiate a cyber strike — managing the entire execution from the tactical event horizon via the C4ISR abilities of the OCS kit. This is only one way in which current and emerging technologies and tactics would be modified to function in a five-dimensional world. This scenario could be as little as two years from reality.

As the world hurtles toward an all-digital society, the US military will need to be able to integrate physical activities with a fusion of wearable devices and technologies. Recently fielded in the aircraft manufacturing industry for precision adjustments and positive identification of individual pieces for a "digital match," such things as Google Glasses heads-up displays and wrist computers make an immediate case for the dismounted operator.[82] Wearables give a hands-free ability to manage difficult tasks in quick succession, while maintaining a send-receive link for streaming information. These technologies take advantage of the unique digital signatures of physical objects in the interconnected network of the IoT.

In an IoT-based scenario running through hand-held cyber tools described for this COA, an AFSOC individual embedded in the SOF ground team would be equipped with wearables that turns this individual into a five-dimensional object. That is, this individual would be able to send and receive streaming data, become a beacon and a sensor, and be able to find, fix, track, target, engage, and assess (F2T2EA) physical and cyber personas by using a variety of signals existing in the IoT. These signals would be plotted by using mapping strategies like those at NGA's cyber team, and then visualized using emerging technologies like DARPA's Plan X as described earlier in this paper. The result would be an actual depiction of the cyber world, with physical objects such as smart phones, smart buildings, and smart cars also visualized as cyber objects with

unique signatures. With this cyber terrain mapped and visualized, a target system analysis would be generated as is done for the physical world, to associate the key nodes to generate the desired effect against the target. In essence, the principles of EBAO, creating effects based on the commander's intent, can be applied to a fully mapped and visualized cyber terrain, just as it is for kinetic targeting in the physical plane.

A scenario that reflects true five-dimensional thinking might run like this: SOF mission planners have been tracking a known terrorist for months. Charts have been drawn up to depict this individual's movements across the area of operations, wire diagrams have traced all his known associates, interviews and human sources have confirmed his terrorist activity, and a case against this individual has been presented to the JAG for targeting as a High Value Individual, or HVI. Along with traditional ISR collection, cyber collection has also mapped out this HVI's persona, network, nodes, and habits. Charts have been drawn up to depict the HVI's movements within cyberspace, wire diagrams have traced all the cyber personas with whom the HVI is associated, and sources have confirmed the unique digital signatures not only of this individual, but also of all his physical objects — his car, his handsets, his microwave, his alarm clock, everything that belongs to him.

Continuing this scenario, an entity like an AFSOC Cyber Attack Team, or CAT, begins planning an effects-based operation against this HVI, using a mixture of physical and non-physical effects against this HVI. The CAT integrates cyber effects into the mission planning phase to precisely hit certain functions or nodes within the cyber map of this HVI, based on the physical and non-physical target system analysis drawn up on this target. Once the mission plan is approved by the mission commander and the JAG, the CAT prepares the hand-held and wearable devices of the JTAC on the team with pre-loaded "apps" the ground team will need

during the mission, just as rifles are locked and loaded, and aircraft munitions are loaded up prior to mission execution.

Continuing the illustration, the ground team is ready to deploy. When required in the pre-planned mission steps, the JTAC pushes a button on a cuff device to mask the digital signature of the team as they go in close to the target. In addition, within the wearables suite, the team carries sensors to triangulate cyber signatures and transmit data back to the CAT or operations center. As the team sets up their perimeter, the JTAC checks in to verify sensor triangulation with other platforms in the area of operations, and reviews this collated SIGINT and FMV data on the JTAC's universal tactical display screen. In this way, the cyber signatures become extremely accurate, with a lower probability of error than an airborne sensor. With a visualization of the cyber signatures all around the team displayed on either a heads-up display such as Google Glasses, or a screen display such as the OCS, the JTAC can filter and hone in on the desired object — the HVI's alarm clock, doorbell, or security system.

According to the mission plan, positive identification of the HVI will be initiated by exploiting the room sensors within the security system of the HVI's home. To do so, the JTAC pushes a button and launches the pre-loaded app to hack the camera system and confirm the location of individuals within the home or compound. After determining a digital match to the HVI's alarm clock, the JTAC initiates a cyber effect by pushing another button — an app to set off the alarm clock. The individual's face is revealed to the hacked cameras, and a digital match is made with the HVI target package on the JTAC's screen.

At this point in the scenario, the team would move out on a target with a cyber activity alert, having found the active IP or signature of the HVI and confirmed the identity of the target. The JTAC cues an aircraft onto the target for a kinetic fires solution, and uses a cyber app to assess the battle damage of the strike. Conversely, the JTAC can initiate a cyber fires event by

pushing a button. In this case, the cyber fires message travels through the uplink carried on the wearables suite to an NSA agent at the operations center, or to the CAT which is live on the net and a virtual member of the team every step of the way — and the pre-planned cyber effect happens upon command. Essentially, this puts the C2 and initiation of cyber actions directly into the hands of an operator on the ground. That is truly tactical cyber, a foot-mobile solution as effective as a bullet or an airstrike delivered on target.

COMPARISON OF RESULTS

Analysis

This paper explores three alternative solutions to enable AFSOC to provide the SOF operator with a range of cyber options in a successful strategy for today's cyber terrain. Three mission-essential criteria are used as an objective standard of measurement to weigh each possible COA, provide a clear assessment, and give pros and cons for their implementation. These three criteria are: cost-effectiveness, C2 capability while forward-deployed, and portability. Taken together, these three criteria prove the feasibility of the COA revealed as AFSOC's best course of action.

COA 1: Cyber Targeting Cells at Operations Centers

In terms of C2, this proposed COA proves its viability by aligning with the existing framework of the TSOC and the authority granted to the geographic combatant commands to plan and direct SOF. Delegating the operational control (OPCON) of theater cyber forces to combatant commanders renders cyber a theater capability rather than a strategic one, and allows a delegated cyber capability a local commander can fully integrate into local planning and operations with a degree of assurance and permanence.[83] This COA assumes the local commander will balance the risks of each cyber-based operation, just as the commander does for all operations. This COA also assumes that the tools for risk assessment will be available to the

local commander, and that strategic targeting will continue to take place at the strategic level while tactical targeting takes place at the tactical level with the local commander.

Placing a SOF cyber team within an existing C2 framework also allows a greater cost-effectiveness. Since the TSOCs already staff and train a cyber subject matter expert, it lies within existing manning and funding channels to use this as a vehicle to grow the capacity to a full JCTC complement.

However, this proposed solution is not truly portable, as the team itself is made up of a number of personnel from USCYBERCOM, NSA, USSOCOM, and each of the Army, Navy, Marines, and Air Force special operations components. This team would best reside at the operations center itself, and at most be able to forward deploy one to two members to a forward location as a forward liaison. The cyber team's computer systems, connectivity, and the ability to reachback to higher headquarters to leverage cyber technologies would not be best served in a forward basing location with degraded or limited communications.

COA 2: Tactical Cyber Authority Decentralized to AFSOC Units

As a cost-effective solution, this proposed COA takes advantage of current programs already underway to put AFSOC into an open architecture framework and push tactical abilities into "apps" useful to operators on the ground. As an example of recent advances that could also be of advantage to trimming the cost, the developmental Plan X Cyberwarfare program referenced earlier aligns with this architectural schema to push cyber down to the tactical level. However, the bill to staff, train, and house additional teams of AFSOC personnel will be a factor.

In consideration of C2, the best way USCYBERCOM can bridge the gap between strategic cyber and tactical cyber is through the Air Force tenant of decentralized execution of air, space, and cyberspace power. This is central to the current employment of AFSOF, as SOF commanders rely on decentralized planning and execution, pushing decisions to the lowest unit

level to ensure the success of dynamic, small-scale special operations conducted by lean, agile teams out in the field.[84] In addition, the liaison activities between the CAT and USSOCOM's JCC via the CTO makes best use of command relationships between AFSOC and USSOCOM to integrate cyber into every aspect of Joint mission planning. Therefore, this COA makes the best case in a strong C2 criterion.

Portability is the third criteria, and here this COA performs better than the other two alternatives. With the construct of a virtual shooter, it may be that the only item to be carried is a capable communications array. This item is already a part of the Combat Controller and JTAC gear, as outlined previously in this paper — keeping portability at the best level technology can provide without the addition of further gear. To enhance the capability of the CAT to provide sensitive real-time cyber solutions to the battlefield without adding weight, the addition of low probability of intercept (LPI) technology software in the communications suite would reduce the possibility of interception and enemy hacking by using burst transmission, or pulses, to keep the live data link in the CCT or JTAC gear protected.[85]

COA 3: Hand-Held Cyber Tools Included in Joint Terminal Attack Controller Gear

As a futuristic solution, this proposed COA has lesser cost-effectiveness than the previous two COAs. However, by leveraging the emerging technologies already underway for AFSOC and the Joint Services in the realm of wearables, heads-up displays, and software suites to visualize all five dimensions of the area of operations, this proposed reality is not so far out of reach.

In terms of C2, the COA described here would use the emerging technologies already paid for and in testing, to provide the critical link between needing a cyber effect to appear on the battlefield, and making it actually happen at the precise time the operator needs it to appear. This is a critical point to enabling a tactical cyber solution. Typical cyber planning takes place

outside the SOF mission planning room, and is delivered to the battlefield at a strategic command level connected to, but not interwoven with, a tactical event. In this COA, as depicted elsewhere in this paper, a hand-held cyber tool for a SOF team member, such as a JTAC, would allow the decentralized execution of a fires event to occur at the initiation of the JTAC, just as it does for a kinetic fires event.

The criterion of portability, as measured against this COA, contains some unknowns. With future technology still in development, finished facts are unavailable, but corollaries can be drawn against current systems. The MTS wearable suite described above weighs approximately 4 pounds.[86] Any changes to this system as it becomes tailored for AFSOC as the Battlefield Air Operations OCS could theoretically add one to two pounds of weight within the processor pack carried on the operator's back. In addition, a notional suite of cyber-focused tools such as Google glasses or a computing cuff device may add one-half to one pound of weight. This additional weight, though slight, makes this COA slightly less portable than the second COA considered.

Results

The Solution to the Problem

After a careful analysis of each alternative to the current state of AFSOC's authority and capability to integrate cyber effects into its mission to support the SOF operator, a single COA emerges as the best solution for AFSOC. Based on the three measurement criteria of cost-effectiveness, C2 capability, and portability, the second COA — to form Cyber Attack Teams for AFSOC at the squadron level — appears as the best way forward for AFSOC to tactically operate in the cyber terrain in the near future.

Today's solution for AFSOC to create a CAT which performs tactical targeting and the release of cyber munitions in direct support of individual SOF missions as a virtual shooter on the team can be applied to each of the Joint Services. For example, the Army recently discussed its efforts to push cyber to operators at the corps level and below in a concept called cyber

electromagnetic activities, or CEMA.[87] The desire of the Army's CEMA is to synchronize cyberspace operations, electronic warfare, and spectrum management operations for the individual operator, which is in line with the proposed scenarios for tactical teams depicted for AFSOC above. Earlier this year, the Marine Corps activated the Marine Corps Cyberspace Warfare Group (MCCYWG) to support USCYBERCOM with both defensive and offensive cyber operations.[88] In a world so interconnected in everything from home security to banking, this new MCCYWG proposes to look at offensive options that take advantage of the intersecting network of the IoT. The Navy, also, is working with USCYBERCOM to create and field cyber mission teams comfortable operating within the cyber terrain and capable of launching offensive cyber weapons for regional combatant commanders.[89] The need for Cyber Attack Teams to bring the authority and capability to execute cyber effects directly at the tactical level is a recognized trend across the conventional Joint Services, and can be a near-term reality for AFSOC and the SOF community.

Vignette of this COA in Action

Putting the principles of this chosen COA to work, a notional vignette would serve to illustrate how to fit together the existing tools and capabilities with a proposed staffing and location plan to launch operational CATs to perform cyber attack missions for AFSOC. To pick up on the HVI example scenario sketched out in the discussion above, a terrorist individual has been tracked to a location, his known associates have been traced, and his cyber signature and behaviors have been identified. As a valid target, this HVI's cyber identifiers have been researched and annotated into the target package in coordination with USSOCOM's JCC to work cyber options into planning strategic and operational objectives, with JSOC as the supported entity for this notional upcoming mission, and with USCYBERCOM for algorithms and

predictive analysis. The involvement of these agencies also exercises the C2 and authorities for AFSOC to plan and execute cyber effects.

In this notional scenario, the mission planning calls for AC-130 gunships. The AFSOC gunship squadron to be involved in the operation begins a mission planning cycle, involving unit-level ISR, operations, and organic CAT personnel. The squadron's CAT pulls up the target folder on this HVI, and sketches out an array of possible cyber effects specific to the upcoming engagement. These cyber effects have been curated on a daily basis by the CAT as part of the team's daily function, keeping in constant conversation with USSOCOM's CTO as the cyber liaison and with USCYBERCOM to ensure the viability of the HVI's cyber signature and the code to affect the HVI's associated cyber network. Like a quiver of cyber arrows, the CAT forges the apps and tools to manipulate the cyber terrain in the area of operations. When mission planning begins, the CAT begins to pick the right arrows for the job. Within an open systems architecture, the CAT pre-loads the apps chosen by the mission commander which the team will use during the operation to launch specific cyber effects at a specific time-on-target.

As the ground team goes in and the operation begins, the CAT is fused to the ground forces via the JTAC's digital interface chosen for this mission. In this way, the CAT becomes a virtual shooter, at weapons-ready. As such, the CAT can react to emerging events on the ground and continuously feed data to the JTAC's display, to include a visual representation of the cyber terrain. In this scenario, the CAT provides real-time tracking of enemy personal devices specific to that mission, while simultaneously, an intelligence squadron at AFSOC provides real-time FMV production, exploitation, and dissemination to the JTAC and to JSOC as the supported command.

From a tactical perspective, the CAT will now begin to shape the actions of the target. Upon command from the JTAC, the CAT will execute an app to send a text message to the HVI,

to shape his actions. These actions would entail making the HVI show up at a time and place of the mission commander's choosing, spoofing a known associate and influencing the HVI to respond and message multiple other contacts, or tipping the HVI to a subordinate's defection — a frame-up created by moving US funds into the subordinate's bank accounts. For this scenario, the CAT causes a text message to be sent to the HVI's hand set influencing the HVI to call in his deputies to his location. The ground team waits for the arrival of the HVI deputies and cross-cues the arriving digital signatures of their handsets or vehicles with the FMV observations to get a digital and visual positive identification of each.

The trigger event occurs. The HVI unlocks his home security to allow the deputies to enter the home or compound. The CAT issues an app command to hack the digital security cameras to track the visual on the movement of the HVI and deputies inside the home. Upon command from the JTAC, the CAT executes a digital mask of the security system, to allow the ground team to move into the building.

The CAT initiates malware upon request or in response to a preplanned time-on-target which affects targeted handsets and other vulnerable lines of communication such as radios. This could take the form of simply degrading devices to increase enemy fog of war at critical moments or could entail a much more sophisticated intent to interject tailored input designed to affect the target organization's response in specific ways.

For this scenario, the CAT hacks into the HVI's iPhone to listen in on his discussion with his deputies without his knowledge, even using the camera to virtually "see" the room and the individuals within it. Next, upon command, the CAT activates the ringers of all the cell phones of the HVI and his deputies, causing the fog of war described above. The CAT also executes a spoofing event to create a digital diversion on the security cameras away from the ground team's location. The team infiltrates the room where the HVI and deputies are located, and conducts the

mission to capture and exfiltrate. The CAT maintains control of the security system, to disallow any alarm from sounding. Upon command, the JTAC orders in the close air support for airborne cover while the ground team completes the exfiltration portion of the operation. As a parting shot, the CAT executes the command to drain the bank account of the HVI, and tell his mistresses about each other.

This scenario illustrates a notional construct wherein a team of cyber attack personnel, whether at AFSOC or any Joint Service, can integrate with mission planning and execution cycles, participate as a virtual shooter on a ground forces team, and provide a tactical means of operating in all five dimensions of the battlefield. The activity of the CAT will be completely driven by the scenario at hand, the ability of US forces to identify and manipulate digital signatures, as well as by what devices the HVI uses — anything from televisions, wristwatches, hand-held radios, vehicles, even rifles and munitions with digital signatures.

RECOMMENDATIONS

AFSOC has the opportunity to put actual cyber effects into AFOSC's capability to support SOF. That capability physically exists, to a varying extent in different theaters. The relationships exist, through the SOCOM Joint Cyber Cell's (JCC) ability to gain mission authorities and mission data from USCYBERCOM and NSA. The process exists, through the JCC framework, requirements generation, and IPL process. To launch this process, this paper recommends that AFSOC investigate and implement the following actions.

Requirements Generation

AFSOC, and indeed all SOF Services, must create documented mission requirements in order to define AFSOC cyber needs, as well as create the funding, staffing, and capability to execute any tactical cyber plan. First, this paper recommends that AFSOC gain more knowledge of cyber initiatives at staff and unit levels. In order to write requirements, those supporting the

SOF mission need to know what cyber can do for them. For example, AFSOC intelligence analysts in unit support missions would benefit from a generalized knowledge of just how cyber can be worked into mission planning as a go-to effect to answer the commander's intent. Courses already exist to create this awareness, and could be a required training item, such as the Joint Cyber Operations Planning Course offered by USCYBERCOM.

Next, AFSOC should gather mission requirements for cyber effects and channel them through the SOCOM J39X cyber office for inclusion into a comprehensive ability for SOCOM to grant ability and authority for the cyber operations AFSOC requests, both defensive and offensive. This action could be drafted at the present time by the A2, A3, and A6 directorates at AFSOC headquarters within the newly created ACT, and, in the future, completed and maintained by the proposed AFSOC Cyber Attack Team (CAT). These two steps would put AFSOC on the road to fully understanding available tactical cyber capabilities, and then to writing them into daily mission requirements down to the unit level.

Training Program Changes

Current AFSOC training scenarios do not fully integrate tactical cyber effects into mission planning activities or ground team exercise execution phases. AFSOC should make it a priority to integrate into USSOCOM exercises with a cyber focus. In fact, AFSOC can take a lead role in pushing for realistic exercise play for tactical cyber effects within its own exercises such as Emerald Warrior, and in Joint and multi-national exercises such as Tempest Wind or Flaming Sword. AFSOC can contribute cyber-mission scenarios to the exercise storyboard, become more involved in the exercise planning cycle, and tie more closely with USSOCOM cyber-based exercise planning activities.

In addition, AFSOC should re-write its Intelligence Formalized Training Unit (IFTU) course material and unit training programs to demonstrate and exercise putting cyber into

AFSOC mission planning. Layering cyber effects into mission planning and response teams should be an activity that takes place in the IFTU capstone exercise, and is carried through follow-on training within the Career Development Course (CDC) construct and individual training records documentation. These practical measures create an awareness of tactical cyber possibilities right from the start of each individual's AFSOC career, making that shift in mindset toward five-dimensional mission planning and execution part of initial training as well as long-term exercises and implementation.

AFSOC Cyber Manning and Readiness

AFSOC currently does not have the staffing and infrastructure to place cyber knowledgeable personnel within the mission planning cells at each unit, or to run one or several CATs to integrate with SOF teams. The recent formation of the ACT, with the participation of the A2, A3, and A6 is grand start. Next, AFSOC's ACT should begin the Integrated Priority List (IPL) process and begin to project a real plan for cyber effects into the fiscal year funding cycle. Engaging in the IPL process would allow the combatant commander to list the highest priority requirements and define shortfalls in AFSOC's cyber program as well as engage recommendations for programming the appropriate funds to step out in the implementation of the COA to create the CAT construct.

In addition to the IPL process, AFSOC should explore Science and Technology (S&T) IPLs, or STIPLs. Once the cyber capability gap has been identified and prioritized, the combatant command can associate technology transition projects with AFSOC's capability gaps, such as the OCS, the Plan X construct, or cyber signature recognition software.

Finally, AFSOC's current ACT should map an approach to creating an AFSOC CAT using the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) method to influence the direction of requirements early in the acquisition

process. This DOTMLPF life cycle would help AFSOC nail down theoretical concepts discussed in this paper and translate them into solid facts, figures, and needs. Thus, this process should explore just how AFSOC can push a button and get a cyber effect to appear on the battlefield at a time and place of its choosing, defend its airborne networks in a remote and austere location, and enable connectivity to forward-deployed teams in network-sparse environments, to name just a few scenarios.

CONCLUSION

Today's battlespace is undergoing a fundamental shift to a five-dimensional environment containing both physical and non-physical features, able to be recognized, tracked, and targeted by tactical operators on the ground or in the air. This paper asked how AFSOC could fulfill its mission to support the SOF operator with a range of cyber options in a world connected by links, nodes, personas, and objects within an emerging and increasingly networked Internet of Things.

As AFSOC steps into this cyber terrain in its supporting mission to SOF, AFSOC will need to have the authorities to execute tactical cyber missions, work closely and easily with its parent organization, USSOCOM, and be able to pull reachback support from CYBERCOM. AFSOC will also require the proper tools and procedures as protective measures to ensure that tactical cyber operations do not quickly become strategic concerns, to include a Collateral Damage Estimate algorithm and modeling software in coordination with a Cyber JMEM to give the best predictions for each offensive cyber action. Thus, AFSOC, and all the SOF Services, can enable the SOF operator to tactically execute cyberwarfare on the front lines by soldiers using cyber-weapons as adeptly as they use live ammunition.

To do so, this paper explored the means by which AFSOC can seize the opportunity to make cyber for SOF a reality, weighing three possible COAs against objective measurement criteria of cost-effectiveness, C2 capability, and portability.

The first COA placed USSOCOM Joint Cyber Targeting Cells, or JCTCs, at operations centers in every theater of operation, streamlining the timeline and authority to strike during ongoing tactical operations by the inclusion of USCYBERCOM individuals in the proposed JCTCs. This COA operates at the Joint level, within the TSOC.

The second COA created Cyber Attack Teams, or CATs, for AFSOC, breaking new ground by making a cyber operator a shooting member of the SOF team. As the "virtual shooter," the CAT remains connected to the ground team throughout the mission, performs tactical targeting, and releases cyber munitions in direct support of individual special operations missions. The CAT concept puts cyber-weapons on the front lines to be tactically executed by ground forces as adeptly as live ammunition. This COA operates at the unit level, within AFSOC units.

The third, and final, COA put hand-held cyber tools into the equipment of AFSOC personnel embedded in the ground forces team. By leveraging emerging and near-term technologies, this COA gives the SOF operator a tactical cyber weapon just as functional as the other weapons carried upon their person. Using wearables, heads-up displays, and software suites to visualize all five dimensions of the area of operations, this proposed reality would allow the decentralized execution of a fires event to occur at the initiation of a SOF team member, such as a JTAC, just as it does for a kinetic fires event. This COA operates at the team level, with individual operators.

This paper judged the second COA as the best means by which AFSOC can launch a comprehensive tactical cyber initiative to support the SOF operator through all five domains. This COA, to create the CAT construct, brings a range of cyber options to the SOF operator in the near-term, while being cost-effective, portable, and capable of clear C2 while forward

deployed. The CAT provides the means for AFSOC, and indeed all SOF Services, to make the comprehensive shift to five-dimensional thinking and operating on the front lines.

This paper concluded with a number of recommendations. AFSOC must create documented mission requirements in order to define cyber needs, as well as create the funding, staffing, and capability to execute any tactical cyber plan. AFSOC should also take a lead role in realistic exercise play for tactical cyber effects and re-write its IFTU course material and unit training programs to teach cyber mission planning.

Finally, AFSOC should take advantage of the emerging shift in five-dimensional thinking by projecting mission funding, methods, and facilities through the vehicles of the IPL process as well as the DOTMLPF method to help AFSOC nail down theoretical concepts discussed in this paper and translate them into solid facts, figures, and needs.

ENDNOTES

[1] LeMay Center for Doctrine, Annex 3-05 Special Operations, "Special Operations Defined," 23 January 2015, 1.

[2] Steve Winterfeld and Jason Andress, The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice, Syngress, 2013, 20.

[3] Air Force Special Operations Command, "Air Force Special Operations Command Factsheet," September 2014.

[4] Air Force Special Operations Command, "AFSOC Cyber Team Mission Statement," May 2016.

[5] Joint Publication 3-12(R), Cyberspace Operations, (Washington DC: GOP, 5 February 2013), II-6-7.

[6] U.S. Department of Defense, "Cyber Command Fact Sheet," 21 May 2010.

[7] Joint Publication 3-0, Joint Operations, (Washington DC: GOP, 11 August 2011), III-3.

[8] Air Force Special Operations Command, "AFSOC Cyber Team Mission Statement," May 2016.

[9] Dr. Mark A. Gallagher and Dr. Michael Horta, "Cyber Joint Munitions Effectiveness Manual (JMEM)," *Modeling & Simulation Journal*, Summer 2013, 5.

[10] National Security Agency, "Frequently Asked Questions - Signals Intelligence (SIGINT)," 3 May 2016.

[11] Joint Publication 3-0, Joint Operations, (Washington DC: GOP, 11 August 2011), III-4.

[12] Patrick Tucker, "Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict," *Defense One*, 29 October 2014.

[13] Ibid.

[14] Christopher Paul, Isaac R. Porche III, and Elliot Axelband, The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces, Arroyo Center, United States Army, Rand Corporation, 2014, 73.

[15] U.S. Department of Defense, "DoD Cyberspace Workforce Framework (DCWF) Overview," February 2016, 3.

[16] Tim Bonds, Army Network-Enabled Operations: Expectations, Performance, and Opportunities for Future Improvements, Arroyo Center, United States Army, Rand Corporation, 2012, 98.

[17] Joint Publication 3-12 (R), Cyberspace Operations, (Washington DC: GOP, 5 February 2013), v.

[18] Ibid, v-vi.

[19] "tactical," *Merriam-Webster.com,* 2016. http://www.merriam-webster.com (16 July 2016).

[20] United Nations, "Internet of Things Global Standards Initiative," 20 July 2015.

[21] David Raymond, et al, "Key Terrain in Cyberspace: Seeking the High Ground," NATO CCD COE Publications, 2014, 290.

[22] Federal Bureau of Investigation, "The Cyber Threat: Part 1: On the Front Lines With Shawn Henry," 27 Mar 2012.

[23] Mark Pomerleau, "State vs. Non-State Hackers: Different Tactics, Equal Threat?," *Defense Systems*, 17 August 2015.

[24] "terrorism," Encyclopædia Britannica.com, 2016. https://www.britannica.com/topic/terrorism (16 July 2016).

[25] P. W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014, 11.

[26] Michael Riley, "Cyber Weapons: The New Arms Race," *Bloomberg Businessweek*, 21 July 2011.

[27] Major Michael Lenart, "The National Military Strategy from a Cyber Perspective," *Military Cyber Affairs*, 12 September 2015.

[28] Matt Lembright, "Protecting the (Cyber) Homeland: The New Age of Cyber Terrorism and Why Force Protection Needs to Embrace Cyberspace," *Military Cyber Affairs*, 9 June 2015.

[29] Major Michael Lenart, "The National Military Strategy from a Cyber Perspective," *Military Cyber Affairs*, 12 September 2015.

[30] Craig Stallard, "At the crossroads of cyber warfare: signposts for the Royal Australian Air Force," Air University (U.S.) School of Advanced Air and Space Studies, 2014, 19.

[31] U.S. Army Training and Doctrine Command, Cyber Operations and Cyber Terrorism, Handbook No. 1.02, 15 August 2005, II-4 - II-7.

[32] U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015.

[33] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, 5.

[34] B. G. J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," United States Cyber Command, 14 August 2012.

[35] *The World's Greatest Air Force, Powered by Airmen, Fueled by Innovation: A Vision for the United States Air Force*, (Washington, DC: Headquarters US Air Force, 10 January 2013), 2.

[36] Joint Publication 1, Doctrine for the Armed Forces of the United States, (Washington DC: GOP, 25 March 2013), III-21.

[37] Jason Address and Steve Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier, 2014, 54.

[38] U.S. Department of Defense, "DoD Cyberspace Workforce Framework (DCWF) Overview," February 2016, 2.

[39] Deborah Bodeau, et al, "Mapping the Cyber Terrain," The MITRE Corporation, Bedford, MA, November 2013, 1.

[40] David Vergun, "Cyber chief: Army cyber force growing 'exponentially'," *US Army*, 5 March 2015.

[41] Defense Advanced Research Projects Agency, Program Information: Plan X. http://www.darpa.mil/program/plan-x

[42] Cheryl Pellerin, "DARPA's Plan X Gives Military Operators a Place to Wage Cyber Warfare," DoD News, Defense Media Activity, 12 May 2016.

[43] GEN Joseph Votel, *Statement of Commander Unites States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., March 18, 2015, 10.

[44] Joint Publication 3-12(R), Cyberspace Operations, (Washington DC: GOP, 5 February 2013), IV-6.

[45] Ibid, III-6.

[46] Ibid, II-7.

[47] Ibid, IV-7.

[48] Mark Martin, "Communicators Come Together for Emerald Warrior's Cyber Phase," Air Force Special Operations Command Public Affairs Bulletin, 9 March 2012.

[49] Air Force Special Operations Command, "AFSOC Cyber Team Mission Statement," May 2016.

[50] Ben FitzGerald and Lt Col Parker Wright, "Digital Theaters: Decentralizing Cyber Command and Control," *Disruptive Defense Papers*, April 2014, 17.

[51] Air Force Special Operations Command, "AFSOC Cyber Team Mission Statement," May 2016.

[52] Ben FitzGerald and Lt Col Parker Wright, "Digital Theaters: Decentralizing Cyber Command and Control," *Disruptive Defense Papers*, April 2014, 11.

[53] U.S. Strategic Command, "U.S. Cyber Command Fact Sheet," March 2015.

[54] U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015.

[55] Ben FitzGerald and Lt Col Parker Wright, "Digital Theaters: Decentralizing Cyber Command and Control," *Disruptive Defense Papers*, April 2014, 5.

[56] Ibid, 6.

[57] Joe Gould, "Former NSA Chief: Follow SOCOM Model for Cyber," *Defense News*, 17 April 2015.

[58] Admiral James Stavridis and David Weinstein, "Time for a US Cyber Force," *Proceedings Magazine*, vol. I/40/I/I, January 2014, 133.

[59] Tim Bonds, Army Network-Enabled Operations: Expectations, Performance, and Opportunities for Future Improvements, Arroyo Center, United States Army, Rand Corporation, 2012, 97-8.

[60] Air Force Special Operations Command, "AFSOC Cyber Team Mission Statement," May 2016.

[61] Air Mobility Command, "Air Mobility Command Factsheet," July 2016.

[62] Air Force Special Operations Command, "Air Force Special Operations Command Factsheet," September 2014.

[63] Ibid.

[64] "tip of the spear," Urban Dictionary.com, 2015. http://www.urbandictionary.com/define.php?term=tip%20of%20the%20spear (29 July 2016).

[65] LeMay Center for Doctrine, Annex 3-05 Special Operations, "AFSOF Operational Planning Considerations," 23 January 2015, 1-2.

[66] Courtney Howard, "Widespread Use of Wearable Technology," *Military and Aerospace Electronics*, 21 September 2015.

[67] Air Force Special Operations Command, "Combat Control Fact Sheet," 1 August 2013.

[68] Donna Miles, "Combat Controllers Play Key Role in Terror War," *American Forces Press Service*, 23 April 2004.

[69] Robert F. Dorr, "The U-28A Quietly Serves SOCOM," *Defense Media Network*, 6 July 2010.

[70] Ben FitzGerald and Lt Col Parker Wright, "Digital Theaters: Decentralizing Cyber Command and Control," *Disruptive Defense Papers*, April 2014, 9.

[71] Ibid, 17.

[72] LeMay Center for Doctrine, Annex 3-30 Command and Control, "Air Operations Center," 7 November 2014, 1-2.

[73] Joint Publication 3-05, Special Operations, (Washington DC: GOP, 16 July 2014), IV-12.

[74] Joint Publication 3-0, Joint Operations, (Washington DC: GOP, 11 August 2011), III-23.

[75] Dr. Mark A. Gallagher and Dr. Michael Horta, "Cyber Joint Munitions Effectiveness Manual (JMEM)," *Modeling & Simulation Journal*, Summer 2013, 5.

[76] Ibid.

[77] LeMay Center for Doctrine, Volume 3 Command, "The Effects-Based Approach to Operations," 5 June 2013.

[78] Patrick Tucker, "Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict," *Defense One*, 29 October 2014.

[79] Black Diamond Advanced Technology, "Modular Tactical System," Accessed 10 August 2016. http://www.bdatech.com/product/mts/

[80] Tamar Eshel, "AFSOC to Equip Dismounted Teams with an Advanced Wearable C4," *Defense Update*, 26 June 2012.

[81] Courtney Howard, "Widespread Use of Wearable Technology," *Military and Aerospace Electronics*, 21 September 2015.

[82] Ibid.

[83] Ben FitzGerald and Lt Col Parker Wright, "Digital Theaters: Decentralizing Cyber Command and Control," *Disruptive Defense Papers*, April 2014, 18.

[84] LeMay Center for Doctrine, Annex 3-05 Special Operations, "AFSOF Command, Control and Organization," 23 January 2015, 3.

[85] Boulat A. Bash, Dennis Goeckel, Saikat Guha, Don Towsley, "Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication," Cornell University, 30 May 2015.

[86] Black Diamond Advanced Technology, "Modular Tactical System," Accessed 10 August 2016. http://www.bdatech.com/product/mts/

[87] David Vergun, "Operators Shift to Cyber Electromagnetic Activities," *US Army*, 5 April 2016.

[88] Sgt. Eric Keenan, "Marine Corps Enters Realm of Cyberspace Through New Unit," *Marines Defense Media Activity*, 25 March 2016.

[89] Joe Gould, "US Navy Cyber Launches Strategic Plan," *Defense News*, 7 May 2015.

BIBLIOGRAPHY

Address, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier, 2014.

Air Force Special Operations Command. *AFSOC Cyber Team Mission Statement*. May 2016.

Air Force Special Operations Command. *Air Force Special Operations Command Factsheet*. September 2014.

Air Force Special Operations Command. *Combat Control Fact Sheet*. 1 August 2013.

Air Mobility Command. *Air Mobility Command Factsheet*. July 2016.

Bash, Boulat A., Dennis Goeckel, Saikat Guha, Don Towsley. "Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication." Cornell University, 30 May 2015.

Black Diamond Advanced Technology. "Modular Tactical System." Accessed 10 August 2016: http://www.bdatech.com/product/mts/

Bodeau, Deborah, et al. *Mapping the Cyber Terrain*. The MITRE Corporation, Bedford, MA, November 2013.

Bonds, Timothy. *Army Network-Enabled Operations: Expectations, Performance, and Opportunities for Future Improvements*. Arroyo Center, United States Army, Rand Corporation, 2012.

Defense Advanced Research Projects Agency. Program Information: Plan X. http://www.darpa.mil/program/plan-x

Dorr, Robert F. "The U-28A Quietly Serves SOCOM." *Defense Media Network*, 6 July 2010.

Eshel, Tamar. "AFSOC to Equip Dismounted Teams with an Advanced Wearable C4." *Defense Update*, 26 June 2012.

Federal Bureau of Investigation. "The Cyber Threat: Part 1: On the Front Lines With Shawn Henry." 27 March 2012.

FitzGerald, Ben and Lt Col Parker Wright. "Digital Theaters: Decentralizing Cyber Command and Control." *Disruptive Defense Papers*, April 2014.

Franz III, B. G. J. "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter." United States Cyber Command. 14 August 2012.

Gallagher, Dr. Mark A. and Dr. Michael Horta. "Cyber Joint Munitions Effectiveness Manual (JMEM)." *Modeling & Simulation Journal*, Summer 2013.

Gould, Joe. “Former NSA Chief: Follow SOCOM Model for Cyber.” *Defense News*, 17 April 2015.

Gould, Joe. “US Navy Cyber Launches Strategic Plan.” *Defense News*, 7 May 2015.

Howard, Courtney. “Widespread Use of Wearable Technology.” *Military and Aerospace Electronics*, 21 September 2015.

Joint Publication 1. Doctrine for the Armed Forces of the United States. Washington DC: GOP, 25 March 2013.

Joint Publication 3-0. Joint Operations. Washington DC: GOP, 11 August 2011.

Joint Publication 3-05. Special Operations. Washington DC: GOP, 16 July 2014.

Joint Publication 3-30. Command and Control of Joint Air Operations. Washington DC: GOP, 10 February 2014.

Joint Publication 3-12(R). Cyberspace Operations. Washington DC: GOP, 5 February 2013.

Keenan, Sgt. Eric. “Marine Corps Enters Realm of Cyberspace Through New Unit.” *Marines Defense Media Activity*, 25 March 2016.

LeMay Center for Doctrine. Annex 3-05 Special Operations. *AFSOF Command, Control and Organization*. 23 January 2015.

LeMay Center for Doctrine. Annex 3-05 Special Operations. *AFSOF Operational Planning Considerations*. 23 January 2015.

LeMay Center for Doctrine. Annex 3-05 Special Operations. *Special Operations Defined.* 23 January 2015.

LeMay Center for Doctrine. Annex 3-30 Command and Control. *Air Operations Center*. 7 November 2014.

LeMay Center for Doctrine. Volume 3 Command. *The Effects-Based Approach to Operations*. 5 June 2013.

Lembright, Matt. “Protecting the (Cyber) Homeland: The New Age of Cyber Terrorism and Why Force Protection Needs to Embrace Cyberspace.” *Military Cyber Affairs*, 9 June 2015.

Lenart, Major Michael . “The National Military Strategy from a Cyber Perspective.” *Military Cyber Affairs*, 12 September 2015.

Martin, Mark. “Communicators Come Together for Emerald Warrior's Cyber Phase.” *Air Force Special Operations Command Public Affairs Bulletin*, 9 March 2012.

Miles, Donna. “Combat Controllers Play Key Role in Terror War.” *American Forces Press Service*, 23 April 2004.

National Security Agency. *Frequently Asked Questions - Signals Intelligence (SIGINT)*. 3 May 2016.

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* Arroyo Center, United States Army, Rand Corporation, 2014.

Pellerin, Cheryl. “DARPA’s Plan X Gives Military Operators a Place to Wage Cyber Warfare.” *DoD News, Defense Media Activity*, 12 May 2016.

Pomerleau, Mark. “State vs. Non-State Hackers: Different Tactics, Equal Threat?” *Defense Systems*, 17 August 2015.

Raymond, David, et al. “Key Terrain in Cyberspace: Seeking the High Ground.” *NATO CCD COE Publications*, 2014.

Revor, Mark S. “Cyber for the middleweight fighter: recommendations for cyberspace capabilities for the United States Marine Corps.” Air University (U.S.) Air War College, 2013.

Riley, Michael. “Cyber Weapons: The New Arms Race.” *Bloomberg Businessweek*, 21 July 2011.

Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

Stallard, Craig. “At the crossroads of cyber warfare: signposts for the Royal Australian Air Force.” Air University (U.S.) School of Advanced Air and Space Studies, 2014.

Stavridis, Admiral James and David Weinstein. “Time for a US Cyber Force.” *Proceedings Magazine*, vol. I/40/I/I, January 2014.

“tactical.” *Merriam-Webster.com*. 2016. http://www.merriam-webster.com (16 July 2016).

“terrorism.” *Encyclopædia Britannica.com.* 2016. https://www.britannica.com/topic/terrorism (16 July 2016).

“tip of the spear.” *Urban Dictionary.com.* 2015. http://www.urbandictionary.com/define.php?term=tip%20of%20the%20spear (29 July 2016).

Tucker, Patrick.“Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict.” *Defense One*, 29 October 2014.

United Nations. *Internet of Things Global Standards Initiative*. 20 July 2015.

U.S. Army Training and Doctrine Command. *Cyber Operations and Cyber Terrorism.* Handbook No. 1.02, 15 August 2005.

U.S. Department of Defense. *Cyber Command Fact Sheet*. 21 May 2010.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. July 2011.

U.S. Department of Defense. *The DoD Cyber Strategy.* April 2015.

U.S. Department of Defense. *DoD Cyberspace Workforce Framework (DCWF) Overview*. February 2016.

U.S. Strategic Command. *U.S. Cyber Command Fact Sheet*. March 2015.

Vergun, David. "Cyber chief: Army cyber force growing 'exponentially'." *US Army*, 5 March 2015.

Vergun, David. "Operators Shift to Cyber Electromagnetic Activities." *US Army*, 5 April 2016.

Votel, GEN Joseph. *Statement of Commander Unites States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., March 18, 2015.

Williams, Major General Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly*, Issue 73, 2nd Quarter, National Defense University Press, April 2014.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Syngress, 2013.